X-SPIErience Day 2020

SOUVERAINETÉ NUMÉRIQUE

SPIE

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
SOUVERAINETÉ NUMÉRIQUE

SPIE

Sécurité OT sans interruption d'activité : gagner en visibilité cyber et minimiser les risques

HUGO CHIFLET

Solution Architect
SPIE ICS

HUBERT RÉMOND

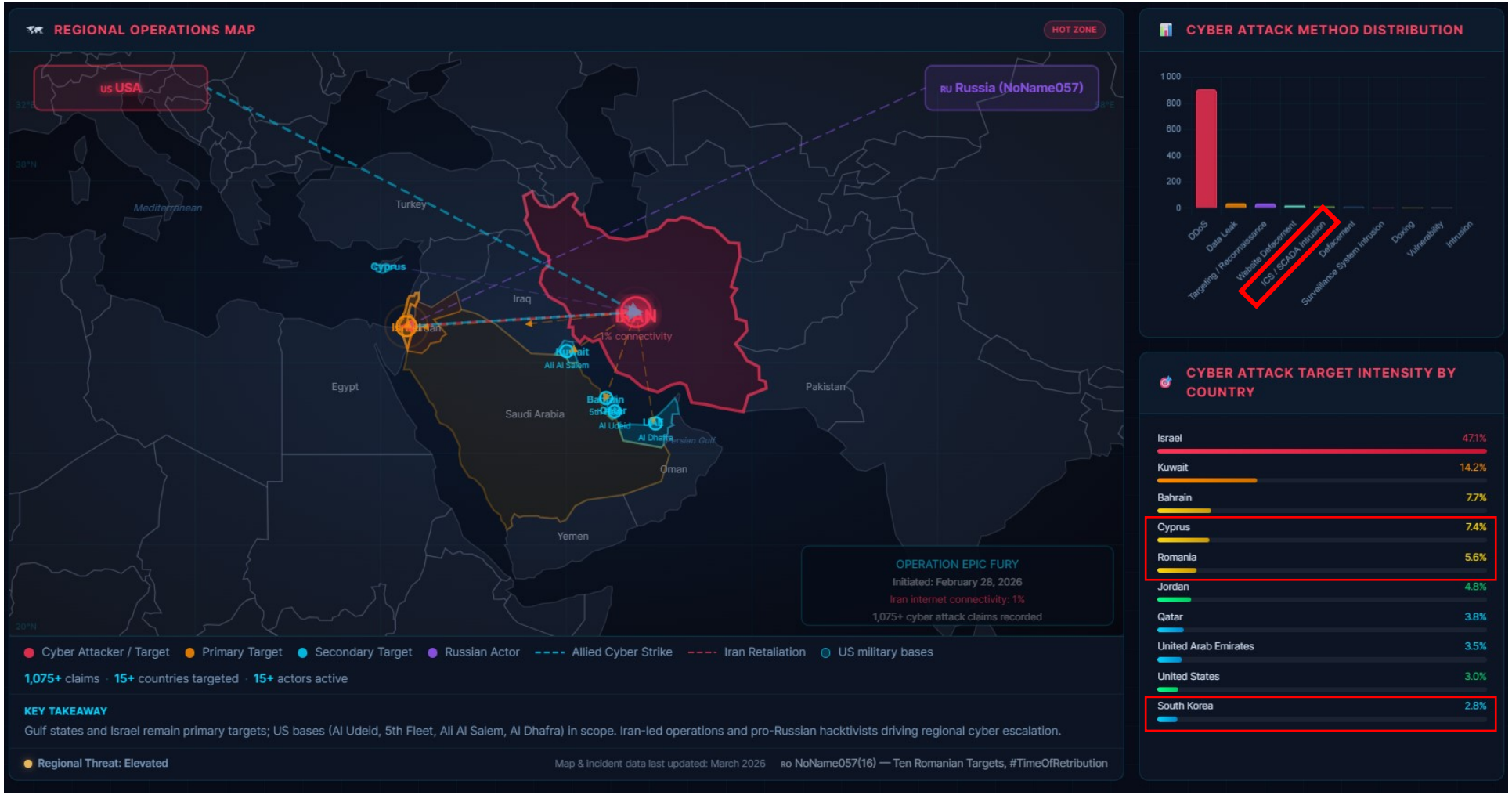
Team Leader Solution
Network Security
SPIE ICS

Lucian Variu

Consultant OT Cybersecurity

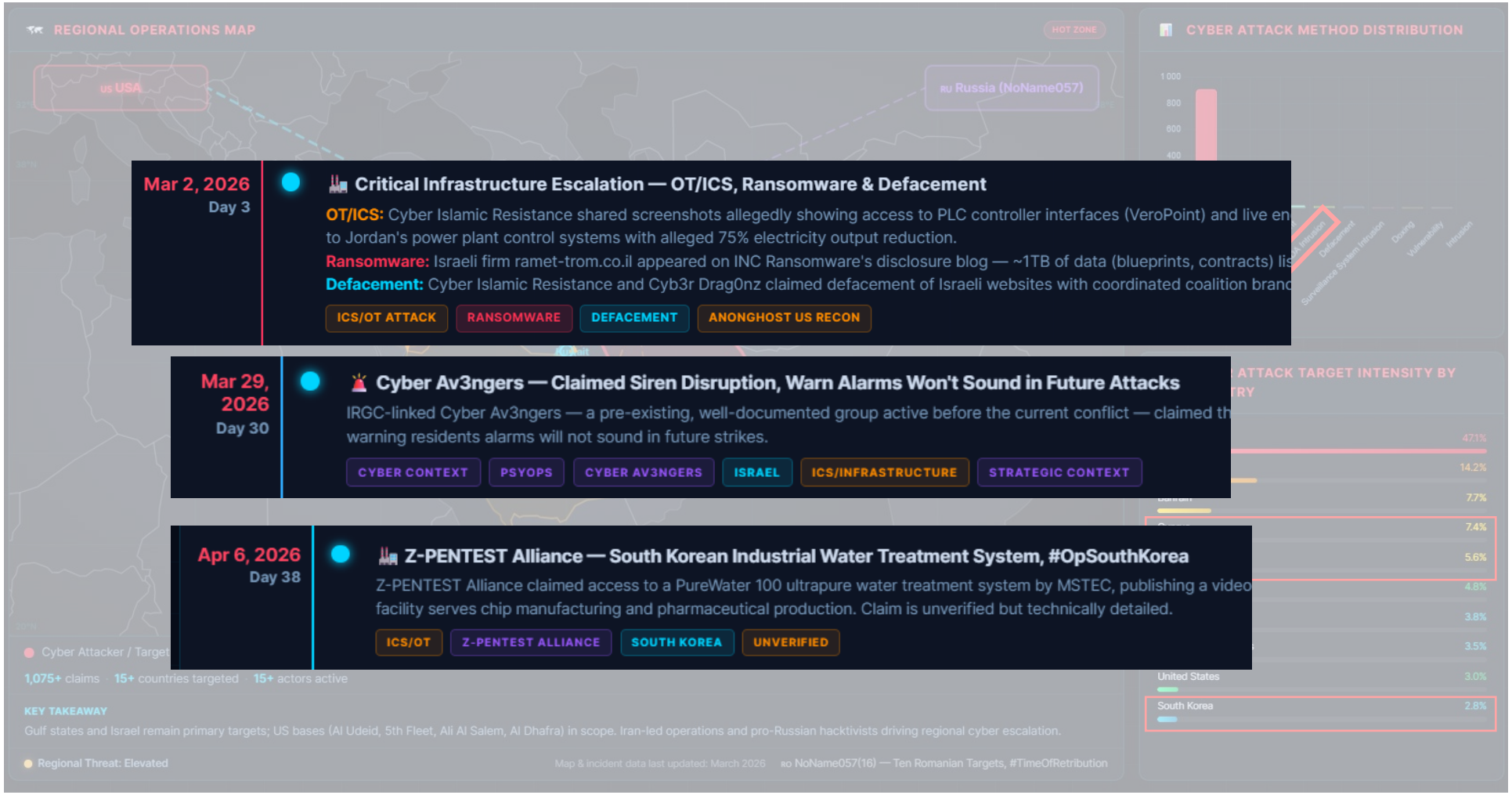
- Mindset orienté sécurité et fiabilité opérationnelle
- Connaissance approfondie des caractéristiques de l'OT
- Solides compétences en collaboration et communication (parlez-moi en FR, DE, EN)
- OT et sécurité industrielle
- IEC 62443-4-1/-3-3
  - Threat modelling
  - Defensible architecture
  - Tabletop exercises (TTX)
  - Secure product development
  - OT visibility and response
  - IT/OT convergence

Paysage actuel des menaces ICS/OT



Source: Iran–Israel/US Cyber War 2026

Paysage actuel des menaces ICS/OT



Source: Iran–Israel/US Cyber War 2026

Paysage des menaces OT en Suisse

SWI swissinfo.ch The Swiss voice in the world since 1935

GEOPOLITICS DEMOCRACY SCIENCE SWISS IDENTITY ECONOMY SWISS ABROAD

News ›

Almost one attack a day reported on critical Swiss infrastructures

The Swiss government received 325 reports of attacks on critical infrastructure last year. Since April 1, 2025, operators of critical infrastructure have been required by law to report cyberattacks within 24 hours.

March 30, 2026 - 14:21

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la cybersécurité OFCS

Meilleure protection des infrastructures critiques en Suisse

18.02.2026 - Le Conseil fédéral veut mieux protéger les infrastructures critiques essentielles à la population suisse et à l'économie contre les défaillances de toutes sortes. Les données électroniques les plus importantes de la Confédération, des cantons et celles relatives aux infrastructures critiques doivent pouvoir bénéficier d'une meilleure protection contre les cyberattaques et la manipulation. Lors de sa séance du 18 février 2026, le Conseil fédéral a donc décidé de faire avancer les travaux relatifs aux projets de loi en réponse à deux motions. Il entend ainsi améliorer la résilience des infrastructures critiques et la sécurité de leurs données.

La motion 23.3001 « Bases légales modernes pour la protection des infrastructures critiques déposée » par la Commission de la politique de sécurité du Conseil des États (CPS-E) demande une révision des bases légales […] **directives contraignantes** en matière de fiabilité et de correction des dysfonctionnements des infrastructures critiques, l'objectif étant **d'augmenter leur résilience** […]

La seconde motion déposée par la CPS-E (23.3002), intitulée « Pour une meilleure sécurité des données numériques essentielles de la Suisse », demande la création de bases légales permettant **d'édicter des directives** à l'intention de la Confédération, des cantons et des exploitants d'infrastructures critiques, dans le but de **mieux protéger les données pertinentes pour la sécurité**.

Sécuriser l'OT | Démo

Introduction au setup

SCENARIO 1

Pas de securité

SCENARIO 2

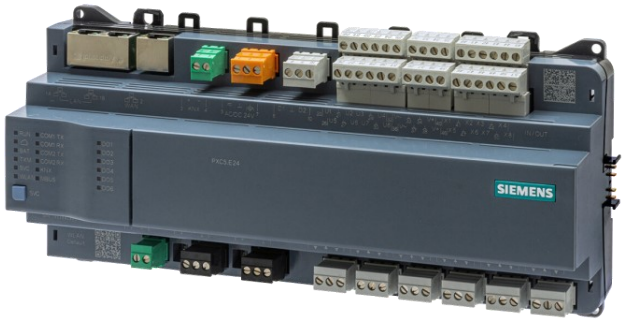
Segmentation PAM & OT Advanced Threat Protection

SCENARIO 3

Honeypot, Advanced Detection & Response

Sécuriser l'OT | Démo

Le contexte



- Un centre de données est refroidi par un système de climatisation
- La température ambiante du centre de données est contrôlée par un PLC Siemens
- Feu vert =  **La température est OK**
- Si la température dépasse 30°C, une alarme est déclenchée =  **Alerte !**
- Le PLC Siemens utilise le protocole BACnet
  - Couramment utilisé pour l'automatisation des bâtiments
  - Communications en clair
  - pas de contrôle d'accès sur BacNet (donc pas de mot de passe ni de contrôle de complexité du mot de passe)

Scenario 1 | Comment ne pas déployer l'OT

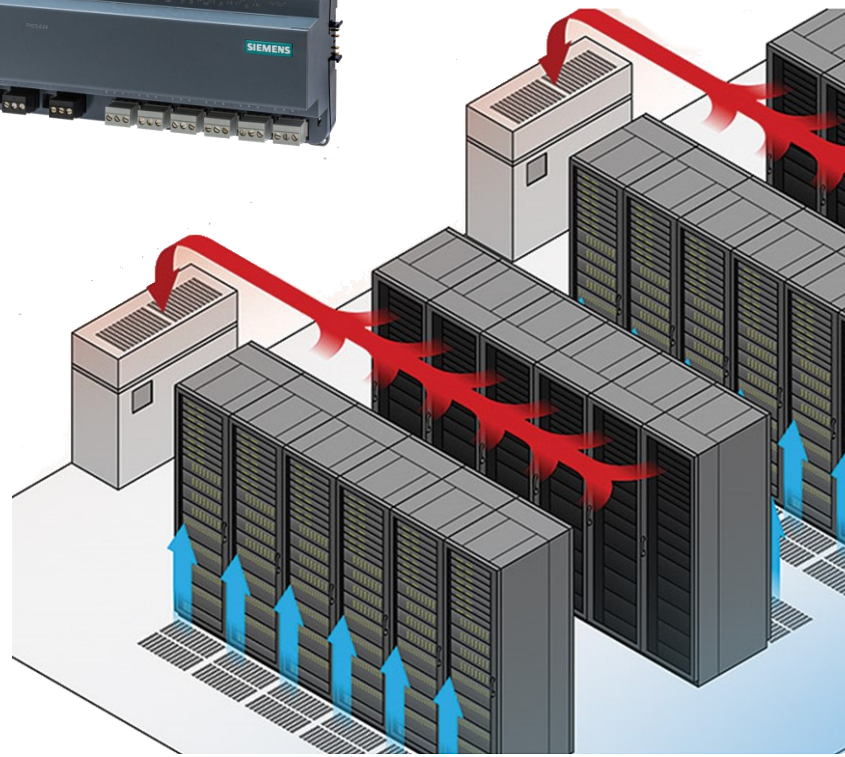
Les équipements :

- Siemens PXC5.E24 PLC
- Commutateur Moxa non géré
- Pas de pare-feu = 1 réseau plat pour l'informatique et l'OT

Software :

- Inneasoft BACnet Explorer
  - aucun contrôle d'accès sur BacNet

Scenario 1 | Comment ne pas déployer l'OT



Scénario :

- Une maintenance standard sur le PLC
- Un technicien en automatisation utilise le logiciel BACnet pour faire passer l'alerte de température de 30°C à 35°C
- Le technicien testera ensuite le système

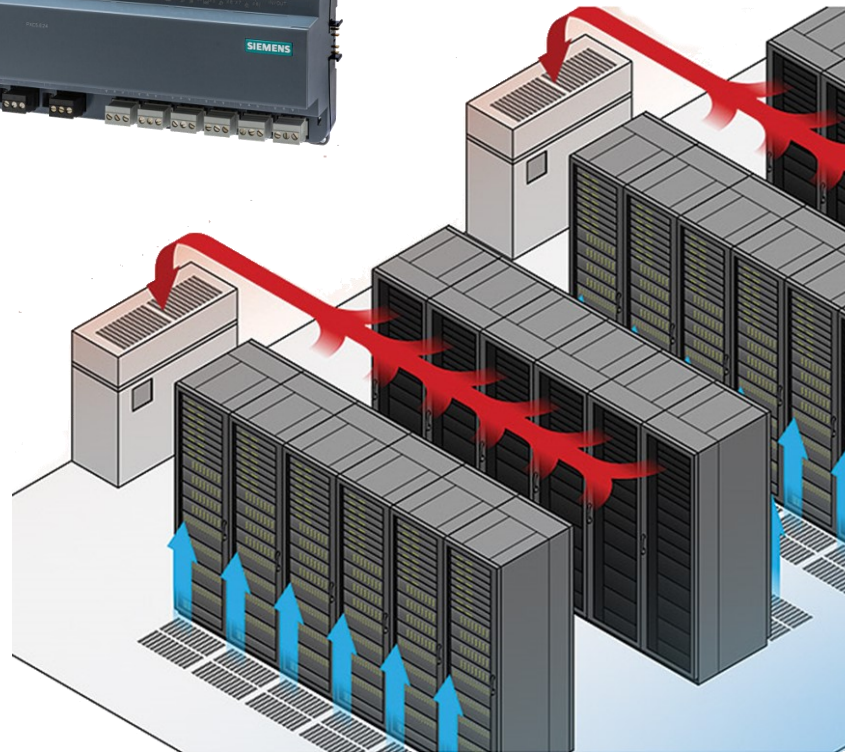
Mise en place :

- Le PLC et les techniciens sont connectés à un commutateur Moxa non géré
- Un seul sous-réseau est utilisé - pas de segmentation ni de sécurité - pas de contrôle d'accès dans la même couche de niveau 2

Scenario 1 | Comment ne pas déployer l'OT

INNEA BACnet EXPLORER

BACnet



Scénario :

- L'objectif de l'attaquant est de provoquer une panne dans le centre de données
- L'attaquant a trouvé un moyen d'accéder au réseau (hôte technicien compromis)
- L'attaquant utilise le même logiciel BACnet pour modifier l'alerte de température et le déclenchement AC à 999°C

Mise en place :

- Même réseau plat

Scenario 2 | Segmentation, PAM & Advanced OT Security

Les équipements :

- Siemens PXC5.E24 PLC

- FortiGate 50G (Rugged) Next-Gen Firewall
- FortiPAM

NEW

NEW

FortiPAM

Software :

- Inneasoft BACnet Explorer
- Fortinet OT IPS/App Ctrl Signatures package

Scenario 2 | Segmentation, PAM & Advanced OT Security

BACnet

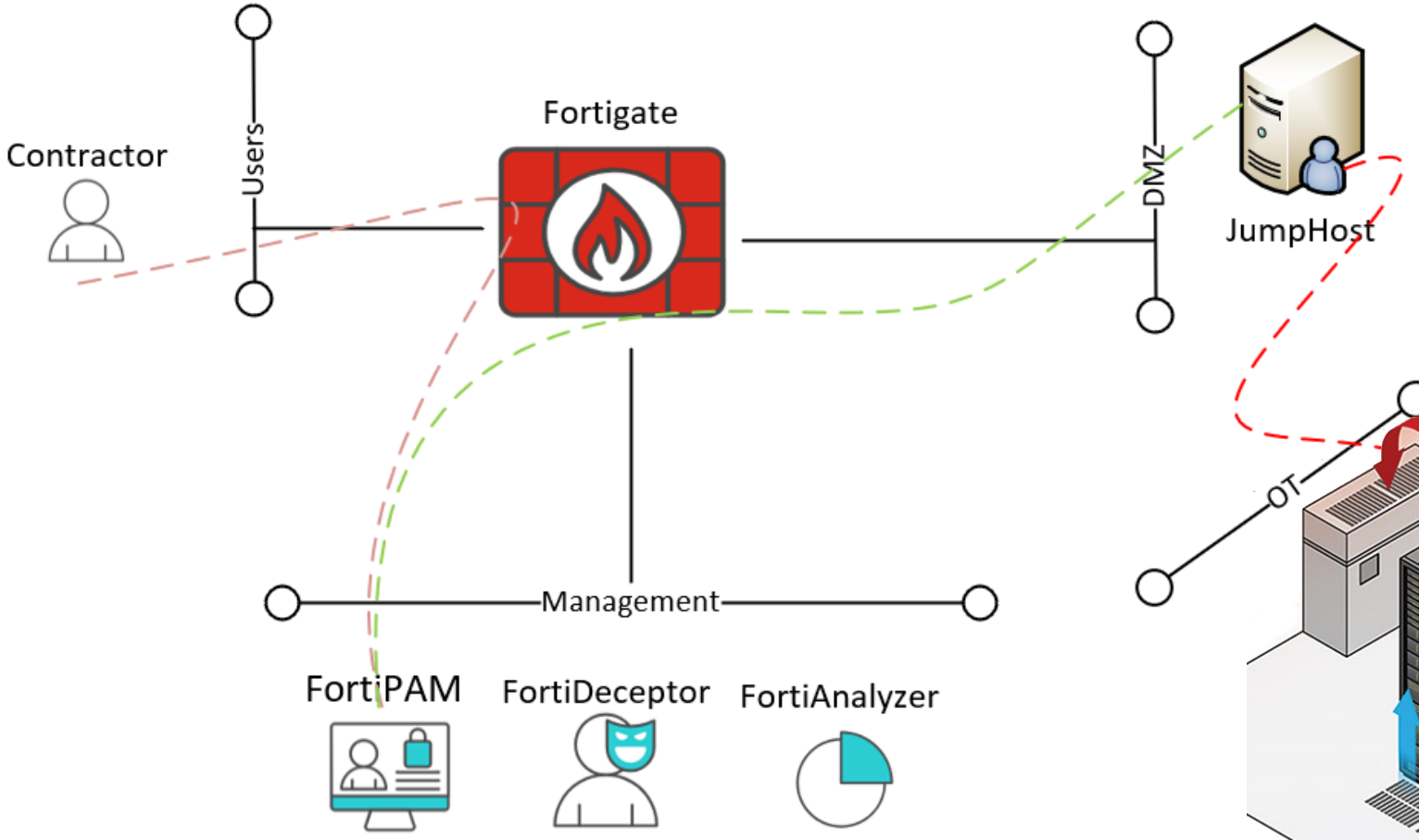
Scénario :

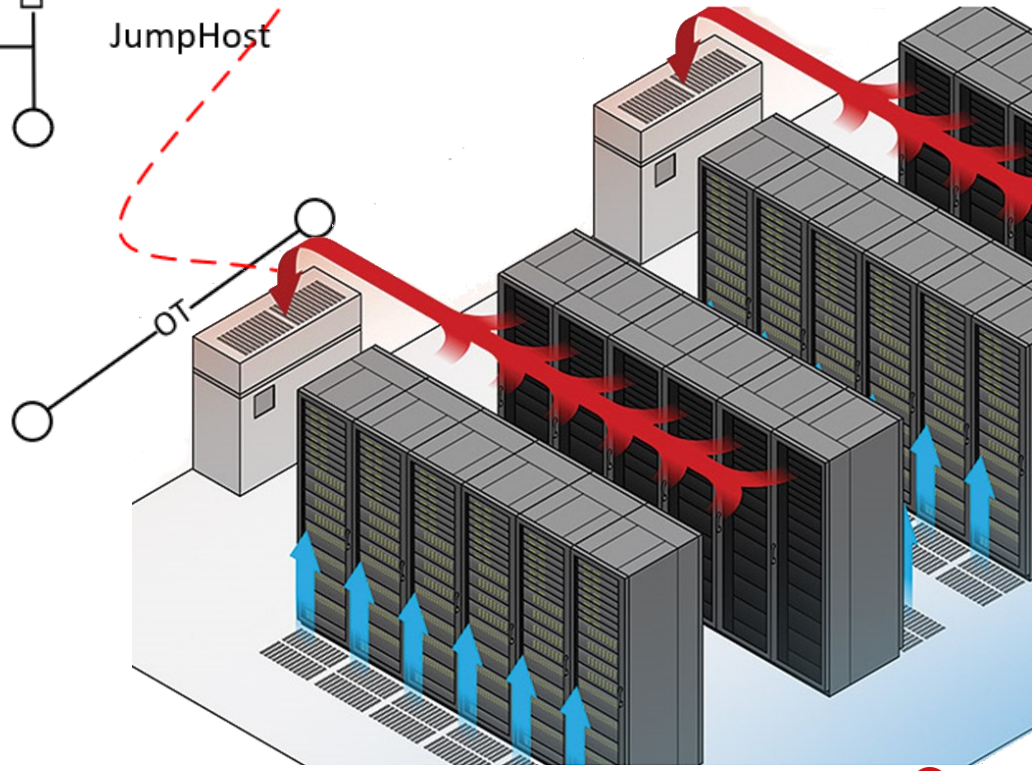
- Identique au scenario 1

Mise en place :

- La segmentation est introduite, avec un VLAN dédié pour le PLC
- La sécurité avancée est appliquée grâce aux signatures IPS OT Fortinet
- L'attaque est bloquée par le pare-feu, la valeur supérieure à 60° pour l'alarme est non autorisée
- L'accès des entrepreneurs peut être sécurisé via FortiPAM

Scenario 2 | Segmentation, PAM & Advanced OT Security





Scenario 3 | Advanced Detection & Response

Les équipements :

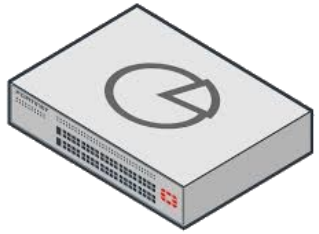
- Siemens PXC5.E24 PLC
- Decoy PLC
- FortiGate 50G (rugged) Next-Gen Firewall
- FortiPAM
- FortiAnalyzer (automated SOC)
- FortiDeceptor (honeypot) NEW

Software :

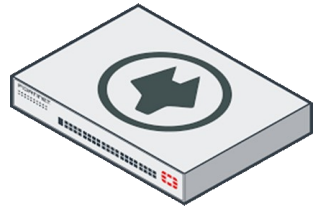
- Inneasoft BACnet Explorer
- Fortinet Security Fabric NEW

FortiPAM

NEW

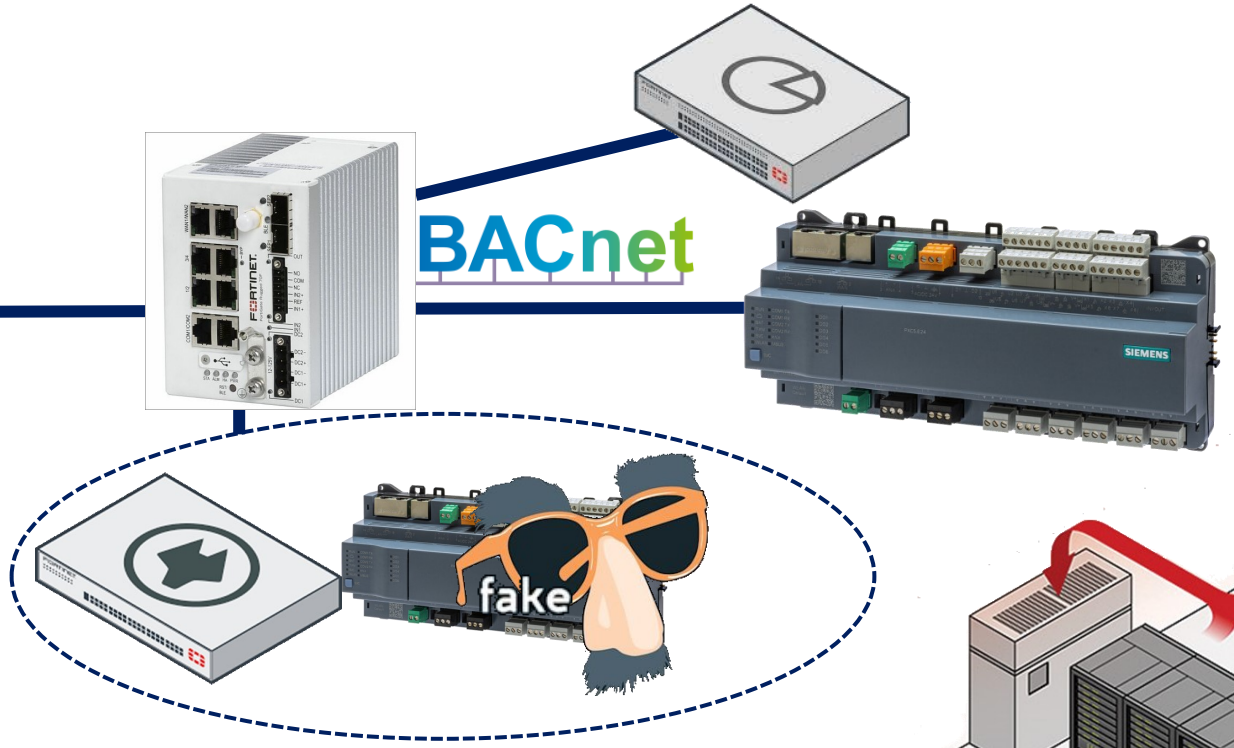


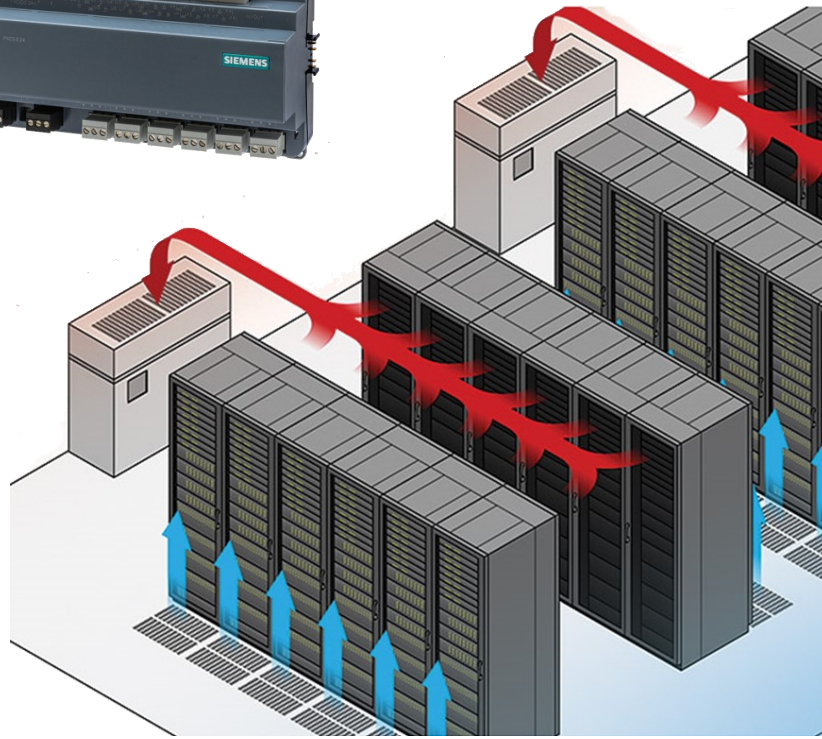
FortiAnalyzer VM



FortiDeceptor VM

Scenario 3 | Advanced Detection & Response





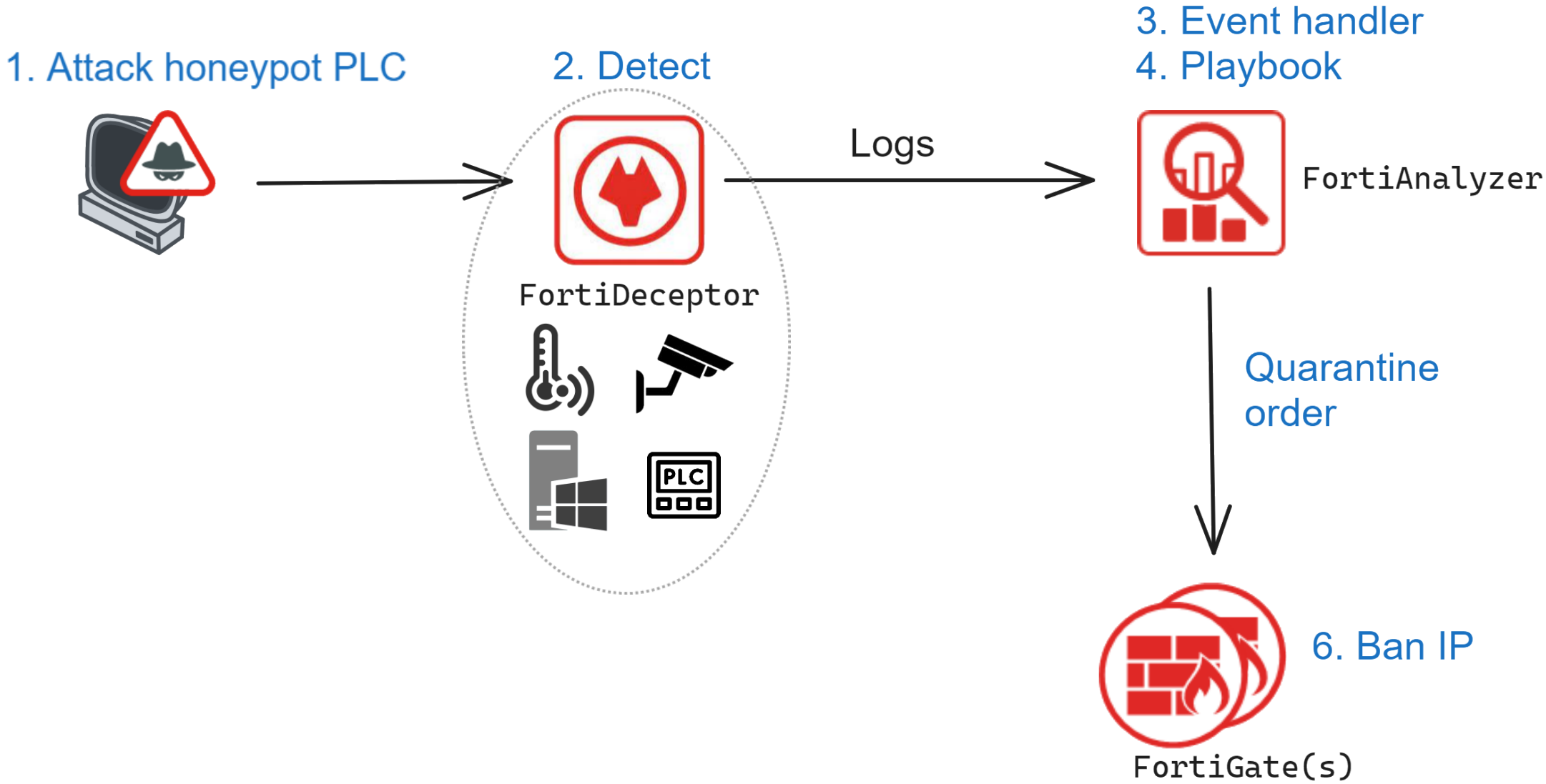
Scénario :

- Notre hacker est de retour
- Mais il ne connaît pas l'IP du PLC
- L'attaquant a scanné le réseau et trouvé un PLC à attaquer
- Il essaiera ensuite de s'y connecter

Mise en place :

- Un faux PLC de leurre est déployé via le FortiDeceptor
- Peut-on voir le hacker et faire quelque chose ?

Scenario 3 | Advanced Detection & Response



Sécuriser l'OT | Conclusion de la Démo

Segmentation (macro et micro) et le **contrôle d'accès** sont essentiels

Utilisez des standards comme **Purdue Model** pour construire votre architecture OT

Le **package dédié de signature OT** offre une protection avancée contre les menaces

Le **pare-feu** et le **commutateur** géré sont le cœur d'un déploiement de sécurité

Le **collecteur de logs** fournit des alertes et des **analyses forensic avancées** en temps réel

Honeypot aide à protéger contre les **mouvements latéraux** et peut détecter et ralentir les attaquants

Automated Security Fabric apporte une **visibilité complète** et une **automatisation** pour sécuriser l'environnement OT

Comment démarrer un projet de cybersécurité OT?

ÉTAPE 1 Rassemblez les bonnes personnes (IT & OT)

ÉTAPE 2 Connaissez votre environnement

ÉTAPE 3 Utiliser des normes reconnues d’architecture de sécurité

ÉTAPE 4 Introduire des solutions de sécurité pertinentes

Vos interlocuteurs chez SPIE ICS

Hugo Chiflet

Solution Architect

Tél. +41 79 862 79 88

Mail hugo.chiflet@spie.com

Hubert Rémond

Team Leader Solution Network Security

Tél. +41 79 801 06 47

Mail hubert.remond@spie.com

spie.ch/cyber